

# SUMS OF TWO SQUARES IN SHORT INTERVALS IN POLYNOMIAL RINGS OVER FINITE FIELDS

EFRAT BANK, LIOR BARY-SOROKER, AND ARNO FEHM

**ABSTRACT.** Landau's theorem asserts that the asymptotic density of sums of two squares in the interval  $1 \leq n \leq x$  is  $K/\sqrt{\log x}$ , where  $K$  is the Landau-Ramanujan constant. It is an old problem in number theory whether the asymptotic density remains the same in intervals  $|n - x| \leq x^\epsilon$  for a fixed  $\epsilon$  and  $x \rightarrow \infty$ .

This work resolves a function field analogue of this problem, in the limit of a large finite field. More precisely, consider monic  $f_0 \in \mathbb{F}_q[T]$  of degree  $n$  and take  $\epsilon$  with  $1 > \epsilon \geq \frac{2}{n}$ . Then the asymptotic density of polynomials  $f$  in the 'interval'  $\deg(f - f_0) \leq \epsilon n$  that are of the form  $f = A^2 + TB^2$ ,  $A, B \in \mathbb{F}_q[T]$  is  $\frac{1}{4^n} \binom{2n}{n}$  as  $q \rightarrow \infty$ . This density agrees with the asymptotic density of such monic  $f$ 's of degree  $n$  as  $q \rightarrow \infty$ , as was shown by the second author, Smilanski, and Wolf.

A key point in the proof is the calculation of the Galois group of  $f(-T^2)$ , where  $f$  is a polynomial of degree  $n$  with a few variable coefficients: The Galois group is the hyperoctahedral group of order  $2^n n!$ .

## 1. INTRODUCTION

An integer  $n$  is a sum of two squares if there exist  $a, b \in \mathbb{Z}$  such that  $n = a^2 + b^2$ . Fermat's theorem characterizes sums of two squares as those integers for which in their prime factorization each prime  $p \equiv 3 \pmod{4}$  appears with even multiplicity. This can be deduced by studying the prime factorization in the ring of Gaussian integers  $\mathbb{Z}[i]$  and noting that  $n$  is a sum of two squares if and only if it is a norm of an element from  $\mathbb{Z}[i]$ . We let

$$(1) \quad b(n) = \begin{cases} 1, & n = a^2 + b^2 \\ 0, & \text{otherwise} \end{cases}$$

be the characteristic function of the set of integers that are a sum of two squares.

**1.1. Landau's Theorem.** A famous theorem of Landau [Lan08] gives the mean value of  $b(n)$ :

$$(2) \quad \langle b(n) \rangle_{n \leq x} := \frac{1}{x} \sum_{n \leq x} b(n) \sim K \frac{1}{\sqrt{\log x}}, \quad x \rightarrow \infty$$

where

$$(3) \quad K = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod{4}} (1 - p^{-2})^{-1/2} \approx 0.764$$

is the Landau-Ramanujan constant. The reader may note the similarity of (2) to the Prime Number Theorem that gives the mean value of the characteristic function of the primes  $\lambda$ :

$$\langle \lambda(n) \rangle_{n \leq x} \sim \frac{1}{\log x}.$$

Indeed, (2) is based on Fermat's theorem, which allows one to express the generating function  $\sum_{n=1}^{\infty} b(n)n^{-s}$  in terms of the Riemann zeta function and the Dirichlet  $L$ -function formed with the non-principal character modulo 4.

**1.2. Sums of Two Squares in Short Intervals.** By (2), the average gap between two consecutive sums of two squares is about  $K^{-1}\sqrt{\log x}$ , hence *naively*, one would expect that if

$$(4) \quad \lim_{x \rightarrow \infty} \frac{\phi(x)}{\sqrt{\log x}} = \infty \quad \text{and} \quad \phi(x) < x,$$

then the mean value of  $b(n)$  in the interval  $\{n \in \mathbb{Z} : |n - x| \leq \phi(x)\}$  is

$$(5) \quad \langle b(n) \rangle_{|n-x| \leq \phi(x)} \sim K \frac{1}{\sqrt{\log x}}, \quad x \rightarrow \infty.$$

The problem of estimating the mean value of  $b(n)$  in such intervals has a long history.

When restricting to all  $x$  but a set of asymptotic density 0, we have the correct upper and lower bounds, up to constants: See Friedlander [Fri82a, Fri82b] and Hooley [Hoo94] for upper bounds; Plaskin [Pla87], Harman [Har91], and Hooley [Hoo94] for lower bounds. See Iwaniec [I76] for the application of the half dimensional sieve to this problem and the exposition [FrI10, §14.3].

For all  $x$ , we have a Maier type phenomenon: Balog and Wooley [BW00] show that for  $\phi(x) = (\log x)^A$ ,  $A > \frac{1}{2}$ , there exist sequences  $x_k^+$  and  $x_k^-$  tending to  $\infty$  such that  $\langle b(n) \rangle_{|n-x_k^{\pm}| \leq \phi(x_k^{\pm})}$  is asymptotically bigger/smaller than what is expected by (5). Thus, (5) cannot be taken so naively, and one must restrict the range (4).

One natural restriction is to  $\phi(x) = x^{\epsilon}$  with fixed  $0 < \epsilon < 1$ . It is a folklore conjecture that (5) should hold; i.e., that for any fixed  $0 < \epsilon < 1$ :

$$(6) \quad \langle b(n) \rangle_{|n-x| \leq x^{\epsilon}} \sim K \frac{1}{\sqrt{\log x}}, \quad x \rightarrow \infty.$$

Using methods of Ingham, Montgomery, and Huxley for primes, one can confirm this conjecture for  $\epsilon > \frac{7}{12}$  unconditionally and for  $\epsilon > \frac{1}{2}$  assuming the Riemann Hypothesis for both the Riemann zeta function and the Dirichlet  $L$ -function formed with the non-principal character modulo 4, see [Hoo74].

**1.3. Landau Theorem in Function Fields.** The classical analogy between number fields and global function fields translates problems about the integers into problems for polynomials over finite fields, see [Rud14] for the classical analogue of the Prime Number Theorem and a survey of some of the recent work in this area. In this note, we will study a function field analogue of sums of two squares in short intervals.

Let  $q$  be an odd prime power and let  $\mathbb{F}_q[T]$  be the ring of polynomials over a finite field  $\mathbb{F}_q$  with  $q$  elements. We denote by  $\mathcal{M}_{n,q} \subseteq \mathbb{F}_q[T]$  the subset of monic polynomials of degree  $n$ . Following [BSW15], the analogue of a sum of two squares that we will consider in this study is a polynomial of the form

$$f = A^2 + TB^2, \quad A, B \in \mathbb{F}_q[T].$$

In other words, we consider norms from the ring  $\mathbb{F}_q[\sqrt{-T}]$ , which we take as the analogue of  $\mathbb{Z}[i]$ . (We could as well study polynomials of the form  $f = A^2 - \alpha TB^2$  with a fixed  $\alpha \in \mathbb{F}_q^\times$ , but in order to keep the presentation simple, we restrict to  $\alpha = -1$ .) We define for  $f \in \mathcal{M}_{n,q}$ :

$$b_q(f) = \begin{cases} 1, & f = A^2 + TB^2 \\ 0, & \text{otherwise.} \end{cases}$$

The analogue of Landau's theorem (2) in function fields should give the asymptotic of the mean value

$$\langle b_q(f) \rangle_{f \in \mathcal{M}_{n,q}} := \frac{1}{\#\mathcal{M}_{n,q}} \sum_{f \in \mathcal{M}_{n,q}} b_q(f)$$

as  $q^n \rightarrow \infty$ . We note that  $q^n$  has several ways to tend to infinity and the asymptotic value is different in different limits, see [BSW15]. In this work we will be interested in the range of parameters when  $q$  is much larger than  $n$ . In this limit, a consequence of a result of the second author, Smilansky, and Wolf [BSW15, Thm. 1.2], says that

$$(7) \quad \langle b_q(f) \rangle_{f \in \mathcal{M}_{n,q}} = \frac{1}{4^n} \binom{2n}{n} + O_n(q^{-1}),$$

where the implied constant depends only on  $n$

**1.4. Sums of Two Squares in Short Intervals in  $\mathbb{F}_q[T]$ .** On  $\mathbb{F}_q[T]$  we have the norm function

$$\|h\| = q^{\deg h} \quad \text{and} \quad \|0\| = 0.$$

Thus, following [KR14], for  $0 < \epsilon < 1$  and  $f_0 \in \mathcal{M}_{n,q}$ , we consider

$$\{f \in \mathbb{F}_q[T] : \|f - f_0\| \leq \|f_0\|^\epsilon\} = \{f_0 + h : h \in \mathbb{F}_q[T], \deg h \leq \epsilon \deg f_0\}$$

as the analogue of  $\{n \in \mathbb{Z} : |n - x| \leq x^\epsilon\}$  in (6). Our main result in this work is a function field analogue of (6) in the limit  $q \rightarrow \infty$ :

**Theorem 1.1.** *For odd  $q$ ,  $n > 2$ ,  $1 > \epsilon \geq \frac{2}{n}$ , and  $f_0 \in \mathcal{M}_{n,q}$  we have*

$$(8) \quad \langle b_q(f) \rangle_{\|f - f_0\| \leq \|f_0\|^\epsilon} = \frac{1}{4^n} \binom{2n}{n} + O_n(q^{-1/2}),$$

where the implied constant depends only on  $n$ .

Note that the error term in (7) is smaller than in (8). However, the method from [BSW15] fails here. For  $\epsilon < \frac{2}{n}$ , (8) no longer holds, as we show in Section 6.

**1.5. Methods.** Our approach is based on the function field analogue of Fermat's theorem [BSW15, Thm. 2.5]:

**Theorem 1.2.** *Let  $f \in \mathcal{M}_{n,q}$ . Then  $b_q(f) = 1$  if and only if in the prime factorization of  $f$ , every prime polynomial  $P \in \mathbb{F}_q[T]$  with  $P(-T^2) \in \mathbb{F}_q[T]$  irreducible appears with even multiplicity.*

In Section 3, we take a ‘generic’ polynomial for the problem,

$$f_{(A_i)}(T) = f_0 + \sum_{0 \leq i \leq \epsilon n} A_i T^i,$$

with the  $A_i$  variables. We use Theorem 1.2 and Galois theory to formulate the property that, under a specialization  $(A_i) \mapsto (a_i)$  of the variable coefficients to elements of  $\mathbb{F}_q$ ,  $b_q(f_{(a_i)}) = 1$ , in terms of the Frobenius element. This, based on an explicit Chebotarev theorem, reduces the proof of Theorem 1.1 to a calculation of the Galois group of  $f_{(A_i)}(-T^2)$ , which we undertake in Section 4 – it turns out to be the hyperoctahedral group of order  $2^n n!$  (cf. Section 2), also known as the Coxeter group of type  $B_n$ , the group of symmetries of the  $n$ -dimensional hypercube.

## 2. THE HYPEROCTAHEDRAL GROUP

We keep in this section to our setting and do not work in full generality to make the exposition as simple as possible.

**Definition 2.1.** Recall that a group  $G$  acting on a set  $\Omega$  is called a *permutation group* if the corresponding map  $G \rightarrow \text{Sym}(\Omega)$  is injective (i.e. no nontrivial element of  $G$  acts trivially on  $\Omega$ ). The regular action of  $G$  on itself (i.e. via multiplication) always makes  $G$  a permutation group.

**Definition 2.2.** Let  $G$  be a permutation group on  $\Omega$  (with left action), let  $C_2 = \{\pm 1\}$  be the cyclic group of order two, and let

$$C_2^\Omega := \{\xi: \Omega \rightarrow C_2\}$$

be the group of functions from  $\Omega$  to  $C_2$ . Then  $G$  acts (from the right) on  $C_2^\Omega$  by

$$\xi^\sigma(\omega) = \xi(\sigma.\omega), \quad \sigma \in G, \omega \in \Omega.$$

The corresponding semidirect product

$$C_2 \wr G := C_2^\Omega \rtimes G$$

is called the (permutational) *wreath product* of  $C_2$  and  $G$ . Its action on  $C_2 \times \Omega$  via

$$(\xi, \sigma).(x, \omega) = (\xi(\sigma.\omega)x, \sigma.\omega), \quad \xi \in C_2^\Omega, \sigma \in G, x \in C_2, \omega \in \Omega$$

makes it a permutation group. In the special case where  $G = S_n$  is the symmetric group acting on  $[n] := \{1, \dots, n\}$ , the group  $C_2 \wr S_n$  is also called the *hyperoctahedral group*.

We introduce a subset  $X_n \subseteq C_2 \wr S_n$  of the hyperoctahedral group that will play a key role in the study that follows:

$$(9) \quad X_n = \left\{ (\xi, \pi) \in C_2 \wr S_n : \prod_{\omega \in \Omega'} \xi(\omega) = 1 \text{ for all orbits } \Omega' \subseteq [n] \text{ of } \pi \right\}.$$

We compute the probability that a randomly chosen element of  $C_2 \wr S_n$  lies in  $X_n$ . For this, recall that a partition  $\lambda \vdash n$  of  $n$  is a tuple  $\lambda = (\lambda_1, \dots, \lambda_n)$  with  $\sum_{j=1}^n j\lambda_j = n$ . The *cycle type* of a permutation  $\pi \in S_n$  is  $\lambda(\pi) := (\lambda_1, \dots, \lambda_n) \vdash n$ , where  $\lambda_j$  is the number of orbits of  $\pi$  of length  $j$ .

**Lemma 2.3.** *We have*

$$(10) \quad \frac{\#X_n}{\#C_2 \wr S_n} = \frac{1}{4^n} \binom{2n}{n}.$$

*Proof.* For each partition  $\lambda \vdash n$ , the number of  $\pi \in S_n$  with cycle type  $\lambda$  is

$$\frac{n!}{1^{\lambda_1} \dots n^{\lambda_n} \cdot \lambda_1! \dots \lambda_n!} = n! \cdot \prod_{j=1}^n \frac{1}{\lambda_j! j^{\lambda_j}},$$

see e.g. [AS11, §14.3]. If  $\pi \in S_n$  has cycle type  $\lambda$ , then out of the  $2^n$  many  $(\xi, \pi) \in C_2 \wr S_n$ , there are

$$\prod_{j=1}^n 2^{(j-1)\lambda_j} = 2^n \cdot \prod_{j=1}^n \frac{1}{2^{\lambda_j}}$$

many in  $X_n$ , as each cycle of  $\pi$  determines one function value of  $\xi$ . Thus,

$$\frac{\#X_n}{\#C_2 \wr S_n} = \frac{1}{n! \cdot 2^n} \cdot \sum_{\lambda \vdash n} \left( n! \cdot \prod_{j=1}^n \frac{1}{\lambda_j! j^{\lambda_j}} \cdot 2^n \cdot \prod_{j=1}^n \frac{1}{2^{\lambda_j}} \right) = \sum_{\lambda \vdash n} \prod_{j=1}^n \frac{1}{\lambda_j! (2j)^{\lambda_j}}.$$

By [KM72, Equation 3] the RHS equals  $\frac{1}{4^n} \binom{2n}{n}$ , as needed. (Indeed, taking a sum over all partitions in [KM72, Equation 3] with  $\theta = 1/2$  one gets on the one hand 1, and on the other hand  $\sum_{\lambda \vdash n} \prod_{j=1}^n \frac{1}{\lambda_j! (2j)^{\lambda_j}} / \frac{1}{4^n} \binom{2n}{n}$ .)  $\square$

### 3. CONNECTION WITH FROBENIUS ELEMENTS

We now work in the following setting: Let  $K$  be a field of characteristic  $\neq 2$  and let  $f \in K[T]$  be a separable polynomial of degree  $n$  such that  $f(0) \neq 0$ . Let  $L$  be a splitting field of  $f$  and let

$$\Omega = \{\omega_1, \dots, \omega_n\} \subseteq L$$

be the set of roots of  $f$ . The Galois group  $G = \text{Gal}(L|K)$  of  $f$  is a permutation group on  $\Omega$ , which gives us an embedding

$$(11) \quad \pi: G \rightarrow S_n, \quad \sigma \mapsto \pi_\sigma$$

that satisfies  $\sigma(\omega_i) = \omega_{\pi_\sigma(i)}$  for all  $\omega \in G$  and  $i \in [n]$ . For each  $i$ , choose two square roots  $\omega_i^\pm = \pm\sqrt{-\omega_i}$  and let  $M = L(\omega_i^\pm : i \in [n])$ . We also denote the map  $\text{Gal}(M|K) \rightarrow S_n$ ,  $\sigma \mapsto \pi_{\sigma|_L}$  by  $\pi$ .

**Lemma 3.1.** *The field  $M$  is the splitting field of the separable polynomial  $f(-T^2)$  and the homomorphism*

$$(12) \quad \Theta: \text{Gal}(M|K) \rightarrow C_2 \wr S_n, \quad \sigma \mapsto (\xi_\sigma, \pi_\sigma),$$

where  $\xi_\sigma: [n] \rightarrow \{\pm 1\}$  is defined by  $\sigma(\omega_i^+) = \xi_\sigma(\pi_\sigma(i))(\sigma\omega_i)^+$  for all  $i$ , equivalently

$$(13) \quad \xi_\sigma(i) = \frac{\sigma((\sigma^{-1}\omega_i)^+)}{\omega_i^+},$$

is an embedding.

*Proof.* The assumptions that  $f(0) \neq 0$  and that  $f$  is separable imply that  $f(-T^2)$  is separable. It is clear that  $M$  is the splitting field of  $f(-T^2)$ . Direct computation shows that  $\Theta$  is a homomorphism, see e.g. [Bar12, Lemma 3.7]. Clearly,  $\Theta$  is injective: If  $(\xi_\sigma, \pi_\sigma)$  is trivial, then  $\sigma\omega_i = \omega_i$  and  $\xi_\sigma(\pi_\sigma(i)) = 1$ , hence  $\sigma(\omega_i^+) = \omega_i^+$  for all  $i$ , and therefore  $\sigma = \text{id}_M$ .  $\square$

**Lemma 3.2.** *The following diagram commutes:*

$$\begin{array}{ccc} \text{Gal}(M|K) & \xrightarrow{\Theta} & C_2 \wr S_n \\ \downarrow & & \downarrow \\ \text{Sym}(\{\omega_i^\pm : i \in [n]\}) & \xrightarrow{\eta} & \text{Sym}(C_2 \times [n]) \end{array}$$

Here the vertical arrows are the embeddings induced by the permutation action,  $\Theta$  is defined in (12), and the isomorphism  $\eta$  is induced from the bijection  $\beta: \{\omega_i^\pm : i \in [n]\} \rightarrow C_2 \times [n]$  given by  $\beta(\omega_i^\pm) = (\pm 1, i)$ .

*Proof.* We have

$$\Theta(\sigma) \cdot \beta(\omega_i^\pm) = (\xi_\sigma, \pi_\sigma) \cdot (\pm 1, i) = (\pm \xi_\sigma(\pi_\sigma(i)), \pi_\sigma(i)) = \beta(\sigma(\omega_i^\pm))$$

for all  $\sigma \in \text{Gal}(M|K)$  and all  $i$ , as claimed.  $\square$

**Lemma 3.3.** *Assume that  $\text{Gal}(M|K) = \langle \phi \rangle$  is cyclic and that  $f$  is irreducible. Then  $f(-T^2)$  is reducible if and only if  $\prod_{i=1}^n \xi_\phi(i) = 1$ .*

*Proof.* Let  $\Theta(\phi) = (\xi, \pi)$ . Since  $f$  is irreducible of degree  $n$  and  $\text{Gal}(M|K) = \langle \phi \rangle$ , we have that  $\text{Gal}(M|L) = \langle \phi^n \rangle$  and  $1, \phi, \dots, \phi^{n-1}$  are representatives of  $\text{Gal}(M|K)/\text{Gal}(M|L) \cong G$ . Moreover, the fact that  $f$  is irreducible implies that  $\pi$  is an  $n$ -cycle.

Since  $\text{Gal}(M|K)$  is abelian,  $L = K(\omega_1)$  and  $M = K(\omega_1^+)$ . In particular,

$$[M : L] = \frac{[M : K]}{[L : K]} \leq \frac{2 \deg f}{\deg f} = 2,$$

and equality holds if and only if  $f(-T^2)$  is irreducible. Hence,

$$\begin{aligned} f(-T^2) \text{ is reducible} & \iff M = L \\ & \iff \omega_1^+ \in L \\ & \iff \phi^n(\omega_1^+) = \omega_1^+ \\ & \iff \xi_{\phi^n}(\pi_{\phi^n}(1)) = 1. \end{aligned}$$

Here, the third line follows by Galois correspondence. Since  $\Theta$  is a homomorphism,

$$(\xi_{\phi^n}, \pi_{\phi^n}) = \Theta(\phi^n) = \Theta(\phi)^n = (\xi, \pi)^n = (\xi \xi^\pi \dots \xi^{\pi^{n-1}}, \pi^n) = (\xi \xi^\pi \dots \xi^{\pi^{n-1}}, 1),$$

so

$$\xi_{\phi^n}(\pi_{\phi^n}(1)) = \prod_{k=0}^{n-1} \xi^{\pi^k}(1) = \prod_{k=0}^{n-1} \xi(\pi^k(1)) = \prod_{i=1}^n \xi(i),$$

where the last equality follows since  $\pi$  is an  $n$ -cycle. Hence,  $f(-T^2)$  is reducible if and only if  $\prod_{i=1}^n \xi(i) = 1$ .  $\square$

The assumption that  $\text{Gal}(M|K)$  is cyclic is satisfied for example when  $K = \mathbb{F}_q$  is a finite field: In that case,  $\text{Gal}(M|K)$  is generated by the  $q$ -Frobenius  $\phi_q(x) = x^q$ .

**Proposition 3.4.** *Let  $q$  be an odd prime power and let  $K = \mathbb{F}_q$ . Let  $f \in K[T]$  be a separable monic polynomial of degree  $n$  with  $f(0) \neq 0$ , and let  $\Theta$  be as in (12). Then  $b_q(f) = 1$  if and only if  $\Theta(\phi_q) \in X_n$ .*

*Proof.* Write  $\Theta(\phi_q) = (\xi, \pi)$  and let  $f = P_1 \cdots P_r$  be the prime factorization of  $f$ . Since  $f$  is separable, i.e. all the  $P_i$ 's are distinct, Theorem 1.2 asserts that  $b_q(f) = 1$  if and only if  $P_i(-T^2)$  is reducible for all  $i$ . The set  $\Omega = \{\omega_1, \dots, \omega_n\}$  of roots of  $f$  is partitioned as  $\Omega = \coprod_{i=1}^r \Omega_i$ , where  $\Omega_i = \{\omega_{k_{i1}}, \dots, \omega_{k_{in_i}}\}$  is the set of roots of  $P_i$ . As each  $P_i$  is irreducible, the sets  $\{k_{i1}, \dots, k_{in_i}\}$  for  $i = 1, \dots, r$  are exactly the orbits of  $\pi$ .

By Lemma 3.3,  $P_i(-T^2)$  is reducible if and only if  $\prod_{j=1}^{n_i} \xi_i(j) = 1$ , where  $(\xi_i, \pi_i) = \Theta_i(\phi_q)$  with  $\Theta_i$  as in (12) for  $P_i(-T^2)$ , that is to say,

$$\Theta_i: \text{Gal}(M_i|K) \rightarrow C_2 \wr S_{n_i},$$

with  $M_i$  the splitting field of  $P_i(-T^2)$ . However, by (13), we have

$$\xi_i(j) = \frac{\phi_q((\phi_q^{-1} \omega_{k_{ij}})^+)}{\omega_{k_{ij}}^+} = \xi(k_{ij}) \quad \text{for } j = 1, \dots, n_i,$$

so we see that  $\prod_{j=1}^{n_i} \xi_i(j) = \prod_{j=1}^{n_i} \xi(k_{ij})$  is the product over the orbit  $\{k_{i1}, \dots, k_{in_i}\}$  of  $\pi$ . We conclude that  $P_i(-T^2)$  is reducible for all  $i$  if and only if  $(\xi, \pi) \in X_n$ .  $\square$

#### 4. THE GENERIC GALOIS GROUP

In this section we compute the Galois group of a suitable generic polynomial.

**Definition 4.1.** Let  $K$  be a field. We say that  $x_1, \dots, x_n \in K^\times$  are *square-independent* if their residues in  $K^\times/(K^\times)^2$  are  $\mathbb{F}_2$ -linearly independent, i.e. if the subspace  $V \subseteq \mathbb{F}_2^n$  consisting of those  $\epsilon = (\epsilon_1, \dots, \epsilon_n) \in \mathbb{F}_2^n$  with

$$\prod_{i=1}^n x_i^{\epsilon_i} \in K^{\times 2}$$

is trivial. Denote

$$w(\epsilon) := \#\{i : \epsilon_i \neq 0\}.$$

The following general lemma is well-known:

**Lemma 4.2.** *For  $n \in \mathbb{N}$ , consider the standard representation of  $S_n$  on  $\mathbb{F}_2^n$ . The only invariant subspaces  $V \subseteq \mathbb{F}_2^n$  are the following:*

- (1)  $V_0 = \{(0, \dots, 0)\}$
- (2)  $V_1 = \{(0, \dots, 0), (1, \dots, 1)\}$
- (3)  $V_{n-1} = \{\epsilon \in \mathbb{F}_2^n : w(\epsilon) \equiv 0 \pmod{2}\}$
- (4)  $V_n = \mathbb{F}_2^n$

*Proof.* If an invariant subspace  $V \subseteq \mathbb{F}_2^n$  is different from  $V_0$  and  $V_1$ , then there exists  $0 \neq \epsilon \in V$  with  $w(\epsilon) < n$ . Applying a suitable transposition  $\sigma \in S_n$ , we get some  $\epsilon' = \epsilon + \sigma\epsilon \in V$  with  $w(\epsilon') = 2$ . This immediately implies that  $V_{n-1} \subseteq V$ , but  $V_n/V_{n-1} \cong \mathbb{F}_2$ , so either  $V = V_{n-1}$  or  $V = V_n$ .  $\square$

**Lemma 4.3.** *Let  $K$  be a field with  $\text{char}(K) \neq 2$  and  $f(T) \in K[T]$  a monic separable polynomial of degree  $n$  with  $f(0) \neq 0$ . Let  $G = \text{Gal}(f(T)|K)$  and let  $\pi : G \rightarrow S_n$  be the embedding  $\sigma \mapsto \pi_\sigma$  defined in (11). Assume that the image  $\pi(G)$  in  $S_n$  has only  $V_0, V_1, V_{n-1}, V_n \subseteq \mathbb{F}_2^n$  as invariant subspaces. Write  $f(T) = \prod_{i=1}^n (T + y_i)$  and let  $L = K(y_1, \dots, y_n)$  be the splitting field of  $f$ . If  $f(0)$  and  $y_1$  are square-independent in  $L$ , then  $\text{Gal}(f(-T^2)|K) \cong C_2 \wr G$ .*

*Proof.* By assumption,  $f(0) = y_1 \cdots y_n$  and  $y_1$  are square-independent in  $L$ . In particular,  $(1, \dots, 1)$  and  $(0, 1, \dots, 1)$  do not lie in the subspace  $V \subseteq \mathbb{F}_2^n$  consisting of those  $\epsilon \in \mathbb{F}_2^n$  with  $\prod_{i=1}^n y_i^{\epsilon_i} \in L^{\times 2}$ , which is  $\pi(G)$ -invariant by assumption. Therefore,  $V = V_0$ , proving that  $y_1, \dots, y_n$  are square-independent in  $L$ .

Hence, by Kummer theory (cf. [Lan02, Ch. VI Thm. 8.1]), if  $M := K(\sqrt{y_1}, \dots, \sqrt{y_n})$  denotes the splitting field of  $f(-T^2)$ , then  $[M : L] = 2^n$ . The image  $H$  of the embedding  $\Theta : \text{Gal}(M|K) \rightarrow C_2 \wr S_n$  of Lemma 3.1 satisfies  $H \leq C_2 \wr \pi(G)$ . Therefore,

$$\#\text{Gal}(f(-T^2)|K) = [M : L] \cdot [L : K] = 2^n \cdot |G| = \#(C_2 \wr G).$$

We conclude that  $\text{Gal}(f(-T^2)|K) \cong C_2 \wr G$ .  $\square$

**Lemma 4.4.** *Let  $K$  be a field with  $\text{char}(K) \neq 2$  and  $f(T) \in K[T]$  a monic polynomial of degree  $n$  with  $\text{Gal}(f(T)|K) \cong S_n$ . Write  $f(T) = \prod_{i=1}^n (T + y_i)$  and let  $L = K(y_1, \dots, y_n)$  be the splitting field of  $f$ . Assume that  $f(0)$  and  $\text{discr}(f)$  are square-independent in  $K$ , and that  $f(0)$  and  $y_1$  are square-independent in  $K(y_1)$ . Then  $f(0)$  and  $y_1$  are square-independent in  $L$ .*

*Proof.* Let  $K_1 = K(y_1)$  and  $f_1(T) = f(T)/(T + y_1) \in K_1[T]$ . Let  $x = f(0)$  and  $y = y_1$ , and suppose that  $x^a y^b \in L^{\times 2}$  with  $a, b \in \{0, 1\}$  and either  $a = 1$  or  $b = 1$ . We identify  $\text{Gal}(L|K)$  with  $S_n$  via the map  $\pi$  given in (11). Since  $\text{Gal}(L|K_1)$  is the stabilizer of  $y$ , it is isomorphic to  $S_{n-1}$ . Therefore, the fixed field  $L_1 = K_1(\sqrt{\text{discr}(f_1)})$  of the alternating group  $A_{n-1}$  is the unique quadratic extension of  $K_1$  inside  $L$  (cf. [Mil14, Corollary 4.2]). So, since  $x^a y^b \notin K_1^{\times 2}$  by assumption, we conclude that  $K_1(\sqrt{x^a y^b}) = L_1$ , or, in other words,

$$x^a y^b \text{discr}(f_1) \in K_1^{\times 2}.$$



Taking the norm  $N = N_{K_1|K}$  in the extension  $K_1|K$ , we get that  $N(x^a y^b \text{discr}(f_1)) \in K^{\times 2}$ . Observe that  $N(x) = x^n$ ,  $N(y) = y_1 \cdots y_n = x$ , and  $N(\text{discr}(f_1)) = \text{discr}(f)^{n-2}$ . Indeed, if we take as representatives for  $S_n/S_{n-1}$  the transpositions  $\tau_k = (1\ k)$  for  $k = 1, \dots, n$ , then

$$N(\text{discr}(f_1)) = \prod_{k=1}^n \text{discr}(f_1)^{\tau_k} = \prod_{k=1}^n \prod_{2 \leq i < j \leq n} (y_{\tau_k(i)} - y_{\tau_k(j)})^2,$$

and each factor  $(y_i - y_j)^2$  with  $1 \leq i < j \leq n$  occurs  $n - 2$  times, namely once for each  $k \notin \{i, j\}$ . Together, we conclude that

$$N(x^a y^b \text{discr}(f_1)) = x^{an+b} \text{discr}(f)^{n-2} \in K^{\times 2}.$$

If  $n - 2$  is odd, then this immediately contradicts the assumption that  $x$  and  $\text{discr}(f)$  are square-independent in  $K$ . Similarly, if  $an + b$  is odd. If both  $n - 2$  and  $an + b$  are even, then  $b = 0$  and thus  $a = 1$ , so  $x \in L^{\times 2}$ , hence  $K(\sqrt{x})$  is the unique quadratic extension of  $K$  inside  $L$ , namely the fixed field  $K(\sqrt{\text{discr}(f)})$  of  $A_n$ , contradicting again the assumption that  $x$  and  $\text{discr}(f)$  are square-independent in  $K$ .  $\square$

**Lemma 4.5.** *Let  $\tilde{f}(T) \in K[T]$  be a separable polynomial and let  $f(T) = \tilde{f}(T) + A \in K(A)[T]$  where  $A$  is transcendental over  $K(T)$ . Then  $\text{discr}(f) \in K[A]$  is not divisible by  $A$ .*

*Proof.* Consider  $g(A) = \text{discr}(f) \in K[A]$ . Since  $\text{discr}(f)$  is a polynomial in the coefficients of  $f$ , we have  $g(a) = \text{discr}(\tilde{f} + a)$  for every  $a \in K$ . In particular,  $g(0) = \text{discr}(\tilde{f}) \neq 0$  since  $\tilde{f}$  is separable, so  $A$  does not divide  $g$ .  $\square$

**Proposition 4.6.** *Let  $F$  be a field of characteristic different from 2, let  $n > m \geq 2$  be integers and let  $f_0 \in F[T]$  be a monic polynomial of degree  $n$ . Define  $K = F(A_0, \dots, A_m)$ , where  $A_0, \dots, A_m$  are independent variables. Then the polynomial*

$$f(T) = f_0(T) + \sum_{i=0}^m A_i T^i \in K[T]$$

*satisfies*

$$\text{Gal}(f(T)|K) \cong S_n \quad \text{and} \quad \text{Gal}(f(-T^2)|K) \cong C_2 \wr S_n.$$

*Proof.* Write  $f_0 = T^n + \sum_{i=0}^{n-1} a_i T^i$ . By replacing  $A_i$  by  $A_i - a_i$ , we may assume without loss of generality that  $a_i = 0$  for  $0 \leq i \leq m$ . In particular,  $f(0) = A_0$ . Applying [BBR15, Proposition 3.6] with  $k = n$  and  $g = 1$  gives that  $\text{Gal}(f(T)|K) \cong S_n$ . In particular,  $\text{discr}(f) \notin K^{\times 2}$ . Write  $f(T) = \prod_{i=1}^n (T + y_i)$ . We will now verify the assumptions of Lemma 4.4.

*Claim 1:*  $f(0)$  and  $\text{discr}(f)$  are square-independent in  $K$

Let  $\tilde{f}(T) = f(T) - A_0 \in K_0[T]$ , where  $K_0 = F(A_1, \dots, A_m)$ , and

$$g(T) = T^{-1} \cdot \tilde{f}(T) = T^{n-1} + a_{n-1} T^{n-2} + \cdots + A_2 T + A_1 \in K_0[T].$$

Since  $g$  is monic and linear in  $A_1$ , it is irreducible in  $K_0[T]$  by Gauss' lemma. Therefore, since  $g(0) = A_1 \neq 0$  and  $g'(0) = A_2 \neq 0$ , both  $g(T)$  and  $\tilde{f}(T) = Tg(T)$  are separable. Thus, by Lemma 4.5,  $\text{discr}(f) \in K_0[A_0]$  is not divisible by  $A_0$ . In particular,

$$A_0 \cdot \text{discr}(f) \notin K^{\times 2}.$$

Together with  $\text{discr}(f) \notin K^{\times 2}$  and the obvious fact that  $A_0 \notin K^{\times 2}$ , we conclude that  $A_0$  and  $\text{discr}(f)$  are square-independent in  $K$ .

*Claim 2:  $f(0)$  and  $y_1$  are square-independent in  $K(y_1)$*

From  $f(-y_1) = 0$  we see that

$$A_1 = -y_1^{-1} \cdot \left( (-y_1)^n + \sum_{i=m+1}^{n-1} a_i(-y_1)^i + \sum_{i=2}^m A_i(-y_1)^i + A_0 \right) \in K_1(y_1),$$

where  $K_1 = F(A_0, A_2, \dots, A_m)$ . Thus,  $K(y_1) = K_1(y_1) = F(A_0, A_2, \dots, A_m, y_1)$ , which, since  $\text{tr.deg}(K(y_1)|F) = m+1$ , implies that  $A_0, A_2, \dots, A_m$  and  $y_1$  are algebraically independent over  $F$  (in other words, the  $(m+1)$ -dimensional hypersurface defined by  $f = 0$  is rational). In particular,  $A_0$  and  $y_1$  are square-independent in  $K(y_1)$ .

*Conclusion of the proof:*

Using Claim 1 and Claim 2, we can now apply Lemma 4.4 and conclude that  $f(0)$  and  $y_1$  are square-independent in the splitting field of  $f(T)$ . Therefore, since  $S_n$  has no invariant subspaces other than the ones of Lemma 4.2, we may invoke Lemma 4.3 and get that  $\text{Gal}(f(-T^2)|K) \cong C_2 \wr S_n$ .  $\square$

## 5. PROOF OF THEOREM 1.1

The proof of Theorem 1.1 follows the pattern of similar proofs in the literature, like in [ABR15, BB15, BBR15, Ent14]. The main ingredient is an explicit Chebotarev theorem, which we recall now.

Fix  $r, d \in \mathbb{N}$  and let  $q$  be a prime power. We let  $\mathbf{A} = (A_1, \dots, A_d)$  be a  $d$ -tuple of variables and define  $R = \mathbb{F}_q[\mathbf{A}]$  and  $K = \mathbb{F}_q(\mathbf{A})$ . For a monic separable polynomial  $g \in R[T]$  of degree  $r$ , we write

$$g(T) = \prod_{i=1}^r (T - \rho_i)$$

and let  $M = K(\rho_1, \dots, \rho_r)$  be a splitting field of  $g$ . We assume that  $M$  is regular over  $\mathbb{F}_q$ , i.e.  $M \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$ , where  $\overline{\mathbb{F}_q}$  is an algebraic closure of  $\mathbb{F}_q$ . The action of  $\text{Gal}(M|K)$  on  $\{\rho_1, \dots, \rho_r\}$  induces an embedding

$$\iota: \text{Gal}(M|K) \rightarrow S_r.$$

For each  $\mathbf{a} = (a_1, \dots, a_d) \in \mathbb{F}_q^d$  we have the homomorphism  $\Phi_{\mathbf{a}}: R \rightarrow \mathbb{F}_q$  given by  $\Phi_{\mathbf{a}}(A_i) = a_i$  for all  $i$ . For those  $\mathbf{a} \in \mathbb{F}_q^d$  which are not a zero of  $\Delta := \text{discr}(g) \in R$ , we can

choose an extension of  $\Phi_{\mathbf{a}}$  to a homomorphism

$$(14) \quad \Phi'_{\mathbf{a}}: R[\Delta^{-1}, \boldsymbol{\rho}] \rightarrow \overline{\mathbb{F}}_q.$$

We apply  $\Phi_{\mathbf{a}}$  to polynomials by applying it to their coefficients. Then

$$g_{\mathbf{a}} := \Phi_{\mathbf{a}}(g) = \prod_{i=1}^r (T - \Phi'_{\mathbf{a}}(\rho_i)) \in \mathbb{F}_q[T],$$

so if  $M_{\mathbf{a}}$  denotes the splitting field of  $g_{\mathbf{a}}$  over  $\mathbb{F}_q$ , then the action of  $\text{Gal}(M_{\mathbf{a}}|\mathbb{F}_q)$  on the set  $\{\Phi'_{\mathbf{a}}(\rho_1), \dots, \Phi'_{\mathbf{a}}(\rho_r)\}$  of roots of  $g_{\mathbf{a}}$  (which has again  $r$  elements since  $\Delta(\mathbf{a}) \neq 0$ ) induces an embedding

$$\iota_{\mathbf{a}}: \text{Gal}(M_{\mathbf{a}}|\mathbb{F}_q) \rightarrow S_r.$$

As before we denote by  $\phi_q \in \text{Gal}(M_{\mathbf{a}}|\mathbb{F}_q)$  the  $q$ -Frobenius.

**Theorem 5.1.** *There exists a constant  $c$  depending only on  $d$  and the total degree of  $g$  (as a polynomial in  $A_1, \dots, A_d, T$ ) such that for every  $X \subseteq \text{Gal}(M|K)$  invariant under conjugation,*

$$\left| \#\{\mathbf{a} \in \mathbb{F}_q^d : \Delta(\mathbf{a}) \neq 0 \text{ and } \iota_{\mathbf{a}}(\phi_q) \in \iota(X)\} - \frac{\#X}{\#\text{Gal}(M|K)} \cdot q^d \right| \leq cq^{d-1/2}.$$

*Proof.* This is classical. In this form of uniformity it can be deduced immediately from [ABR15, Theorem A.4].  $\square$

*Proof of Theorem 1.1.* Let  $q$  be an odd prime power,  $n > 2$ ,  $1 > \epsilon \geq \frac{2}{n}$ ,  $f_0 \in \mathcal{M}_{n,q}$ , and put  $m = \lfloor \epsilon n \rfloor \geq 2$ . We let  $\mathbf{A} = (A_0, \dots, A_m)$  be a tuple of independent variables and define  $K = \mathbb{F}_q(\mathbf{A})$ . Let

$$f(T) = f_0(T) + \sum_{i=0}^m A_i T^i \in K[T]$$

and

$$g(T) = (-1)^n \cdot f(-T^2) \in K[T].$$

Now let  $L$  be the splitting field of  $f$  over  $K$ , write  $f = \prod_{i=1}^n (T - \omega_i)$  and let  $\Omega = \{\omega_1, \dots, \omega_n\} \subseteq L$ . For each  $i = 1, \dots, n$  choose a square root  $\rho_i = \sqrt{-\omega_i}$  and let  $\rho_{n+i} = -\rho_i$ . Then

$$g(T) = \prod_{i=1}^{2n} (T - \rho_i)$$

and  $M = K(\boldsymbol{\rho})$  is the splitting field of  $g$ . Let  $\Theta: \text{Gal}(M|K) \rightarrow C_2 \wr S_n$  be the homomorphism given in (12). By Proposition 4.6,  $\text{Gal}(L|K) \cong S_n$  and  $\Theta$  is an isomorphism. As Proposition 4.6 also applies to  $F = \overline{\mathbb{F}}_q$  instead of  $F = \mathbb{F}_q$ , we get that  $\text{Gal}(M\overline{\mathbb{F}}_q|K\overline{\mathbb{F}}_q) = \text{Gal}(M|K)$ , and therefore  $M|\mathbb{F}_q$  is regular.

The discriminant  $\Delta := \text{discr}(g)$  is a non-zero polynomial in  $\mathbf{A}$  of degree  $\leq 4n$  (by the resultant formula). Therefore,

$$(15) \quad \#\{\mathbf{a} \in \mathbb{F}_q^{m+1} : \Delta(\mathbf{a}) = 0\} \leq 4nq^m,$$

see e.g. [Sch76, Ch. 4 Lemma 3A].

For  $\mathbf{a} \in \mathbb{F}_q^{m+1}$  which is not a zero of  $\Delta$  we choose a homomorphism  $\Phi'_{\mathbf{a}}$  as in (14) and let  $f_{\mathbf{a}} := \Phi_{\mathbf{a}}(f), g_{\mathbf{a}} := \Phi_{\mathbf{a}}(g) \in \mathbb{F}_q[T]$ . Note that

$$f_{\mathbf{a}}(T) = \prod_{i=1}^n (T - \Phi'_{\mathbf{a}}(\omega_i))$$

and

$$g_{\mathbf{a}}(T) = (-1)^n \cdot f_{\mathbf{a}}(-T^2) = \prod_{i=1}^{2n} (T - \Phi'_{\mathbf{a}}(\rho_i)),$$

so  $\Omega_{\mathbf{a}} := \{\Phi'_{\mathbf{a}}(\omega_1), \dots, \Phi'_{\mathbf{a}}(\omega_n)\}$  is the set of zeros of  $f_{\mathbf{a}}$ ,  $L_{\mathbf{a}} = \mathbb{F}_q(\Phi'_{\mathbf{a}}(\omega))$  is a splitting field of  $f_{\mathbf{a}}(T)$ , and  $M_{\mathbf{a}} = \mathbb{F}_q(\Phi'_{\mathbf{a}}(\rho))$  is a splitting field of  $f_{\mathbf{a}}(-T^2)$ . Let

$$\Theta_{\mathbf{a}} : \text{Gal}(M_{\mathbf{a}}|\mathbb{F}_q) \rightarrow C_2 \wr S_n$$

be as in (12) and  $\iota_{\mathbf{a}} : \text{Gal}(M_{\mathbf{a}}|\mathbb{F}_q) \rightarrow S_{2n}$  as above. By Lemma 3.2, the following diagram commutes:

$$(16) \quad \begin{array}{ccccc} \text{Gal}(M|K) & \xrightarrow{\Theta} & C_2 \wr S_n & \xleftarrow{\Theta_{\mathbf{a}}} & \text{Gal}(M_{\mathbf{a}}|\mathbb{F}_q) \\ & \searrow \iota & \downarrow & \swarrow \iota_{\mathbf{a}} & \\ & & S_{2n} & & \end{array}$$

Now let  $X_n \subseteq C_2 \wr S_n$  be as in (9) and define  $X := \Theta^{-1}(X_n) \subseteq \text{Gal}(M|K)$ . By Proposition 3.4,  $b_q(f_{\mathbf{a}}) = 1$  if and only if  $\Theta_{\mathbf{a}}(\phi_q) \in X_n$ . The commutativity of (16) shows that the latter is equivalent to  $\iota_{\mathbf{a}}(\phi_q) \in \iota(X)$ .

Therefore, Theorem 5.1 applied to  $g$  with  $r = 2n$  and  $d = m + 1$ , together with (15), gives a constant  $c_n$  depending only on  $m, n$  and the total degree of  $g$  such that

$$(17) \quad \left| \# \{ \mathbf{a} \in \mathbb{F}_q^{m+1} : b_q(f_{\mathbf{a}}) = 1 \} - \frac{\#X}{\#\text{Gal}(M|K)} \cdot q^{m+1} \right| \leq c_n q^{m+1/2}.$$

Since  $m \leq n$  and the total degree of  $g$ , which equals  $2n$ , are independent of  $q$  and the choice of the polynomial  $f_0$  of degree  $n$ , the constant  $c_n$  can be chosen to depend only on  $n$ . Plugging (10) into (17) concludes the proof.  $\square$

## 6. SMALL $\epsilon$

In this section we deal with  $0 < \epsilon < \frac{2}{n}$ . These  $\epsilon$ 's are not covered by Theorem 1.1. We construct sequences of  $f_0 = f_{0,q_i} \in \mathcal{M}_{n,q_i}$  of a fixed arbitrarily large degree  $n$  such that  $\langle b_{q_i}(f) \rangle_{\|f-f_0\| \leq \|f_0\|^\epsilon}$  asymptotically differs from (8) as  $q_i \rightarrow \infty$ . This shows that the restriction on  $\epsilon$  in Theorem 1.1 is not redundant.

**6.1. First interval:**  $0 < \epsilon < \frac{1}{n}$ . Let  $q$  be an odd prime power. We fix  $k \geq 1$  and let  $n = 2k + 1$  and  $f_0 = T^{2k+1}$ . Then

$$\{f \in \mathbb{F}_q[T] : \|f - f_0\| \leq \|f_0\|^\epsilon\} = \{T^{2k+1} + a : a \in \mathbb{F}_q\}.$$

We note that  $b_q(T^{2k+1} + a) = 1$  if and only if  $a$  is a square in  $\mathbb{F}_q$ . Indeed, if  $b_q(T^{2k+1} + a) = 1$ , then  $T^{2k+1} + a = A^2 + TB^2$ , so  $a = A(0)^2$  is a square and if  $a = b^2$  with  $b \in \mathbb{F}_q$ , then  $T^{2k+1} = b^2 + T(T^k)^2$ , so  $b_q(T^{2k+1} + a) = 1$ .

There are exactly  $\frac{q+1}{2}$  squares in  $\mathbb{F}_q$ , thus

$$\langle b_q(f) \rangle_{\|f - f_0\| \leq \|f_0\|^\epsilon} = \frac{(q+1)/2}{q} = \frac{1}{2} + \frac{1}{2q},$$

which is obviously not compatible with (8).

**6.2. Second interval:**  $\frac{1}{n} \leq \epsilon < \frac{2}{n}$ . Fix a prime  $p > 2$ , let  $n = p^2$ ,  $\nu \in \mathbb{N}$ ,  $q = p^{2\nu}$ , and  $f_0 = T^{p^2} \in \mathbb{F}_q[T]$ . We compute the asymptotic mean value of  $b_q(f)$  for  $f$  in

$$\{f \in \mathbb{F}_q[T] : \|f - f_0\| \leq \|f_0\|^\epsilon\} = \{T^{p^2} + a_1T + a_0 : a_1, a_0 \in \mathbb{F}_q\}$$

as  $\nu \rightarrow \infty$  (and hence also  $q = p^{2\nu} \rightarrow \infty$ ).

**Theorem 6.1.** *Let*

$$(18) \quad c_p = \frac{1}{2^{p^2} p^2 (p^2 - 1)} + \frac{1}{2^p p^2} + \frac{1}{2^{p^2} (p^2 - 1)} \cdot \sum_{1 \neq d | p^2 - 1} 2^{(p^2 - 1)(d - 1)/d} \phi(d),$$

where  $\phi(d)$  is the Euler totient function. Then

$$(19) \quad \langle b_q(f) \rangle_{\|f - f_0\| \leq \|f_0\|^\epsilon} \sim c_p, \quad \nu \rightarrow \infty.$$

Bounding the last summand for  $d = p^2 - 1$  gives that

$$c_p \geq \frac{1}{2^{p^2} (p^2 - 1)} \cdot 2^{(p^2 - 1) \cdot (p^2 - 2)/(p^2 - 1)} \phi(p^2 - 1) = \frac{1}{4} \cdot \frac{\phi(p^2 - 1)}{p^2 - 1} \gg \frac{1}{\log \log p^2}, \quad p \rightarrow \infty,$$

as  $\phi(n) \gg \frac{n}{\log \log n}$  for  $n \rightarrow \infty$ . On the other hand,

$$\frac{1}{4^{p^2}} \binom{2p^2}{p^2} \sim \frac{1}{\sqrt{\pi p}}, \quad p \rightarrow \infty.$$

Thus, if we pick  $p$  sufficiently large, we see that  $c_p > \frac{1}{4^{p^2}} \binom{2p^2}{p^2}$ , hence (19) is not compatible with (8).

To prove (19), we take the same approach as the one used to obtain (8), namely applying the explicit Chebotarev Theorem (Theorem 5.1); however, the respective Galois groups are different, which explains the different asymptotic formula.

Let  $F|\mathbb{F}_{p^2}$  be a field extension,  $A_0, A_1$  independent variables,  $K = F(A_0, A_1)$  and

$$f(T) = T^{p^2} + A_1 T + A_0 \in K[T].$$

As  $\text{Aut}(\mathbb{F}_{p^2} | F \cap \mathbb{F}_{p^2})$  is trivial, [Uch70, Theorem 2] gives that

$$(20) \quad G := \text{Gal}(f|K) \cong \text{Aff}(\mathbb{F}_{p^2}),$$

the group of affine linear transformations

$$\sigma_{a,b} : x \mapsto ax + b, \quad a \in \mathbb{F}_{p^2}^\times, \quad b \in \mathbb{F}_{p^2}$$

of the affine line  $\mathbb{A}^1(\mathbb{F}_{p^2})$  (the isomorphism being an isomorphism of permutation groups). We start by a few group theoretical properties of  $G$ .

**Lemma 6.2.** *Consider  $G = \text{Aff}(\mathbb{F}_{p^2})$  acting on  $V = \mathbb{F}_2^{p^2}$  via the embedding  $G \rightarrow S_{p^2}$ . Then the  $G$ -invariant subspaces of  $V$  are the same as the  $S_{p^2}$ -invariant subspaces; that is to say, the spaces  $V_0, V_1, V_{p^2-1}, V_{p^2}$  as in Lemma 4.2.*

*Proof.* Let  $U$  be a  $G$ -invariant subspace of  $V$ . We want to apply the results of [Kle75] to  $\mathfrak{G} = G$ ,  $n = p^2$ ,  $\Omega = \mathbb{F}_{p^2} \cong \{1, \dots, n\}$  and the field  $K = \mathbb{F}_2$ . Note that in the notation used there,  $M_1 = V_1$ ,  $M^1 = V_{n-1}$ , and  $M = (M_1 + M^1)/M_1 = (V_1 \oplus V_{n-1})/V_1 \cong V_{n-1}$ , as  $\mathbb{F}_2[G]$ -modules.

Since  $\mathfrak{G}$  contains the transitive subgroup  $\mathfrak{H} := \mathbb{F}_{p^2}$  for which 2 does not divide the order of the stabilizer  $\mathfrak{H}_a = 1$  for  $a \in \Omega$ , [Kle75, Hilfssatz 7(b)] gives that

$$(21) \quad U \subseteq V_{n-1} \quad \text{or} \quad V_1 \subseteq U.$$

Moreover, since  $\mathfrak{G}$  is 2-transitive on  $\Omega$ ,  $2 \nmid n$ , and the stabilizer  $\mathfrak{G}_a = \mathbb{F}_{p^2}^\times$ , for  $a = 0 \in \Omega$  contains the subgroup  $\tilde{\mathfrak{H}} := \mathfrak{G}_a$ , which is transitive on  $\Omega_a = \Omega \setminus \{a\}$  and satisfies  $2 \nmid |\tilde{\mathfrak{H}}_b| = 1$  for  $b \in \Omega_a$ , [Kle75, Satz 8(b)] gives that  $V_{n-1}$  is simple. Thus,  $U \cap V_{n-1} = V_0$  or  $U \cap V_{n-1} = V_{n-1}$ .

If  $U \cap V_{n-1} = V_0$ , then  $\dim U \leq 1$  and by (21) we conclude that either  $U = V_0$  or  $V_1 \subseteq U$  and therefore  $U = V_1$ . If  $U \cap V_{n-1} = V_{n-1}$ , then we conclude from  $V/V_{n-1} \cong \mathbb{F}_2$  that either  $U = V_{n-1}$  or  $U = V_n$ .  $\square$

For an element  $\sigma_{a,b} \in G$  we let  $\lambda(\sigma_{a,b}) := (\lambda_1, \dots, \lambda_{p^2}) \vdash p^2$  be the cycle type of  $\sigma_{a,b}$ .

**Lemma 6.3.** *Let  $a \in \mathbb{F}_{p^2}^\times$ ,  $b \in \mathbb{F}_{p^2}$  and  $\sigma = \sigma_{a,b}$ .*

- (a) *If  $a = 1$  and  $b = 0$ , then  $\lambda(\sigma) = \lambda^0 := (p^2, 0, \dots, 0)$ .*
- (b) *If  $a = 1$  and  $b \neq 0$ , then  $\lambda(\sigma) = \lambda^{p^+} := (0, \dots, 0, p, 0, \dots, 0)$ .*
- (c) *If  $a \neq 1$  has multiplicative order  $d$ , then  $\lambda(\sigma) = \lambda^{d^\times} := (1, 0, \dots, 0, \frac{p^2-1}{d}, 0, \dots, 0)$ .*

*Proof.* (a) and (b) are trivial.

Let  $a \neq 1$  be of multiplicative order  $d$ . Then  $x = 0$  is the unique fixed point of  $\sigma_{a,0}$ . For each  $x \neq 0$ , the orbit of  $x$  is  $\{x, ax, \dots, a^{d-1}x\}$  and is of length  $d$ . So we have exactly  $\frac{p^2-1}{d}$  orbits of length  $d$ . This implies that  $\lambda(\sigma_{a,0}) = \lambda^{d^\times}$ . Since  $\sigma_{a,b}$  is conjugated to  $\sigma_{a,0}$ , we get that in fact  $\lambda(\sigma_{a,b}) = \lambda^{d^\times}$  for all  $b$ , as was needed for (c).  $\square$

**Proposition 6.4.** *Let  $p > 2$  be prime,  $F|\mathbb{F}_{p^2}$  a field extension,  $A_0$  and  $A_1$  independent variables, and  $K = F(A_0, A_1)$ . Then the polynomial*

$$f(T) = T^{p^2} + A_1 T + A_0$$

*satisfies*

$$\text{Gal}(f(T)|K) \cong \text{Aff}(\mathbb{F}_{p^2}) \quad \text{and} \quad \text{Gal}(f(-T^2)|K) \cong C_2 \wr \text{Aff}(\mathbb{F}_{p^2}).$$

*Proof.* Write  $f(T) = \prod_{i=1}^{p^2} (T + y_i)$ , so that  $L = K(y_1, \dots, y_{p^2})$  is a splitting field of  $f$ . Let  $K_1 = K(y_1)$ . Since  $0 = f(-y_1)$ , we have

$$(22) \quad A_0 = (y_1^{p^2-1} + A_1)y_1.$$

Thus,  $K_1 = F(A_0, A_1, y_1) = F(A_1, y_1)$ . Since the transcendence degree of  $K_1$  over  $F$  is 2, this implies that  $K_1$  is the field of rational functions in  $A_1, y_1$  over  $F$ .

As  $f'(T) = A_1$ , we get that

$$\text{discr}(f) = \pm \prod_{i=1}^{p^2} \prod_{j \neq i} (y_i - y_j) = \pm \prod_{i=1}^{p^2} f'(y_i) = \pm A_1^{p^2}.$$

So, as  $p^2$  is odd,  $\text{discr}(f)$  is not a square in  $K_1$ , hence  $L_1 := K_1(\sqrt{\text{discr}(f)}) = K_1(\sqrt{\pm A_1})$  is a quadratic extension of  $K_1$  that is contained in  $L$ .

Since  $\text{Gal}(L|K_1)$  is a stabilizer in  $G = \text{Aff}(\mathbb{F}_{p^2})$  of a point  $x \in \mathbb{F}_{p^2}$ , which, without loss of generality, we may choose to be  $x = 0$ , we have  $\text{Gal}(L|K_1) \cong \mathbb{F}_{p^2}^\times$ . As  $\mathbb{F}_{p^2}^\times$  is cyclic,  $K_1$  has a unique quadratic extension inside  $L$  which by the previous paragraph is  $L_1$ .

By Lemmas 4.3 and 6.2, it suffices to prove that  $A_0 = f(0)$  and  $y_1$  are square-independent in  $L$ . Assume on the contrary that  $A_0^a y_1^b \in (L^\times)^2$  for some  $a, b \in \{0, 1\}$  with either  $a = 1$  or  $b = 1$ . Note that since  $K_1$  is a rational function field in  $A_1, y_1$ , (22) implies that  $A_0, y_1$  are square-independent in  $K_1$ , so  $A_0^a y_1^b \notin (K_1^\times)^2$ . Thus  $K_1(\sqrt{A_0^a y_1^b})$  is a quadratic extension of  $K_1$  that is contained in  $L$ , so it must be equal to  $L_1$ . Thus by (22),

$$\pm A_0^a y_1^b A_1 = \pm (y_1^{p^2-1} + A_1)^a y_1^{a+b} A_1 \in (K_1^\times)^2,$$

which leads to a contradiction, as  $K_1$  is a rational function field in  $A_1, y_1$ , and  $A_1 + y_1^{p^2-1}$ ,  $y_1$ , and  $A_1$  are co-prime in  $F[A_1, y_1]$ .  $\square$

*Proof of Theorem 6.1.* Let  $q = p^{2\nu}$ ,  $f(T) = T^{p^2} + A_1 T + A_0$  and  $G = \text{Aff}(\mathbb{F}_{p^2})$ . Since by Proposition 6.4 the Galois group of  $g(T) := f(-T^2)$  is  $C_2 \wr G$  both over  $\mathbb{F}_q(A_0, A_1)$  and over  $\overline{\mathbb{F}}_q(A_0, A_1)$ , the same line of arguments as in the proof of Theorem 1.1 gives that

$$(23) \quad \langle b_q(f) \rangle_{\|f-f_0\| \leq \|f_0\|^\epsilon} \sim \frac{\#(X_{p^2} \cap C_2 \wr G)}{\#(C_2 \wr G)},$$

as  $\nu \rightarrow \infty$ . By Lemma 6.3, the number  $N_\lambda$  of elements of  $G$  of cycle type  $\lambda$  is

$$N_\lambda = \begin{cases} 1, & \lambda = \lambda^0, \\ p^2 - 1, & \lambda = \lambda^{p^+}, \\ p^2 \phi(d), & \lambda = \lambda^{d \times}, 1 \neq d \mid p^2 - 1, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, as we saw in the proof of (10), one has

$$\begin{aligned}
 \#(X_{p^2} \cap C_2 \wr G) &= \sum_{\lambda \vdash p^2} N_\lambda \prod_{j=1}^{p^2} 2^{\lambda_j(j-1)} \\
 (24) \qquad \qquad \qquad &= 1 + (p^2 - 1)2^{p(p-1)} + p^2 \sum_{1 \neq d \mid p^2-1} \phi(d) 2^{(d-1)(p^2-1)/d}.
 \end{aligned}$$

Since  $\#(C_2 \wr G) = 2^{p^2} p^2 (p^2 - 1)$ , by (24) it follows that  $\frac{\#(X_{p^2} \cap C_2 \wr G)}{\#(C_2 \wr G)} = c_p$  (with  $c_p$  defined in (18)), and thus by (23), the proof is done.  $\square$

#### ACKNOWLEDGEMENTS

The authors are grateful to Alexei Entin for suggesting to them the characterization of sums of squares in terms of the Frobenius, to Peter Müller for pointing them to the paper of Klemm, and to Ron Peled for introducing the Ewens sampling formula to them.

The first author was partially sponsored by the Shulamit Aloni Grant for promoting women in science of the Israeli Ministry of Science, Technology and Space no. 3-11924 and the first and second authors by a grant of the Israel Science Foundation no. 952/14. The third author was supported by a research grant from the Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg.

#### REFERENCES

- [AS11] R.B.J.T. Allenby and Alan Slomson. *How to count. An introduction to combinatorics*. Second Edition, Taylor and Francis, 2011. 2
- [ABR15] Julio C. Andrade, Lior Bary-Soroker, and Zeev Rudnick. Shifted convolution and the Titchmarsh divisor problem over  $\mathbb{F}_q[t]$ . *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, Theo Murphy meeting issue ‘Number fields and function fields: coalescences, contrasts and emerging applications’ compiled and edited by J. P. Keating, Z. Rudnick and T. D. Wooley, 373(2040), 2015. 5, 5
- [BW00] Antal Balog and Trevor D. Wooley. Sums of two squares in short intervals. *Canad. J. Math.* 52(4):673–694, 2000. 1, 2
- [BB15] Efrat Bank and Lior Bary-Soroker. Prime polynomial values of linear functions in short intervals. *J. Number Theory* 151:263–275, 2015. 5
- [BBR15] Efrat Bank, Lior Bary-Soroker, and Lior Rosenzweig. Prime polynomials in short intervals and in arithmetic progressions. *Duke Math. J.* 164(2):277–295, 2015. 4, 5
- [Bar12] Lior Bary-Soroker. Irreducible values of polynomials. *Adv. Math.* 229(2):854–874, 2012. 3
- [BSW15] Lior Bary-Soroker, Yotam Smilansky, and Adva Wolf. On the function field analogue of Landau’s theorem on sums of squares. arXiv:1504.06809, 2015. 1.3, 1.4, 1.5
- [Ent14] Alexei Entin. On the Bateman-Horn conjecture for polynomials over large finite fields. arXiv:1409.0846, 2014. 5
- [Fri82a] J. B. Friedlander. Sifting short intervals. *Math. Proc. Cambridge Philos. Soc.* 91(1):9–15, 1982. 1.2
- [Fri82b] J. B. Friedlander. Sifting short intervals. II. *Math. Proc. Cambridge Philos. Soc.* 92(3):381–384, 1982. 1.2



- [Fri10] John Friedlander and Henryk Iwaniec. *Opera de cribro*. American Mathematical Society Colloquium Publications, 57. American Mathematical Society, Providence, RI, 2010. xx+527 pp. ISBN: 978-0-8218-4970-5 [1.2](#)
- [Har91] Glyn Harman. Sums of two squares in short intervals. *Proc. London Math. Soc.* (3) 62(2): 225–241, 1991. [1.2](#)
- [Hoo74] Christopher Hooley. On the intervals between numbers that are sums of two squares. III. *J. Reine Angew. Math.* 267(1):207–218, 1974. [1.2](#)
- [Hoo94] Christopher Hooley. On the intervals between numbers that are sums of two squares. IV. *J. Reine Angew. Math.* 452:79–109, 1994. [1.2](#)
- [I76] H. Iwaniec. The half dimensional sieve. *Acta Arith.* 29(1): 69–95, 1976. [1.2](#)
- [KM72] S. Karlin and J. McGregor. Addendum to a paper of W. Ewens. *Theoret. Population Biology.* 3:113–114, 1972. [2](#)
- [KR14] Jonathan P. Keating and Zeév Rudnick. The variance of the number of prime polynomials in short intervals and in residue classes. *Int. Math. Res. Not. IMRN* 2014(1): 259–288, 2014. [1.4](#)
- [Kle75] Michael Klemm. Über die Reduktion von Permutationsmoduln. *Math. Z.* 143:113–117, 1975. [6.2](#), [6.2](#)
- [Lan08] Edmund Landau. Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate. *Arch. Math. Phys.* 13:305–312, 1908. [1.1](#)
- [Lan02] Serge Lang. *Algebra*. Springer, 2002. [4](#)
- [Mil14] James Milne. *Fields and Galois theory*. Lecture notes, version 4.50, 2014. [4](#)
- [Pla87] V. A. Plaksin. The distribution of numbers that can be represented as the sum of two squares. *Izv. Akad. Nauk SSSR Ser. Mat.* 51(4): 860–877, 1987. [1.2](#)
- [Rud14] Zeev Rudnick. Some problems in analytic number theory for polynomials over a finite field. *Proceedings of the ICM vol 1*, 2014. [1.3](#)
- [Sch76] Wolfgang M. Schmidt. *Equations over Finite Fields. An Elementary Approach*. Springer 1976. [5](#)
- [Uch70] Kôji Uchida. Galois group of an equation  $X^n - aX + b = 0$ . *Tohoku Math. J. (2)*, 22(4):670–678, 1970. [6.2](#)

RAYMOND AND BEVERLY SACKLER SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY,  
TEL AVIV 69978, ISRAEL  
*E-mail address:* [bankefrat@gmail.com](mailto:bankefrat@gmail.com)

RAYMOND AND BEVERLY SACKLER SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY,  
TEL AVIV 69978, ISRAEL  
*E-mail address:* [barylir@post.tau.ac.il](mailto:barylir@post.tau.ac.il)

UNIVERSITÄT KONSTANZ, FACHBEREICH MATHEMATIK UND STATISTIK, FACH D 203, 78457 KON-  
STANZ, GERMANY  
*E-mail address:* [arno.fehm@uni-konstanz.de](mailto:arno.fehm@uni-konstanz.de)